Please replace the paragraph beginning on line 9 of page ~~8~~ 17 with the following amended paragraph: AP 7-14-10

In still another aspect of the present invention, an AES processor adapted to both encryption and decryption is composed of a first selector unit selecting an element of a state in response to row and column indices, an inverse affine transformation circuit applying an inverse affine transformation on the selected element, a second selector unit selecting one out of two data bytes consisting of the selected element received from the first selector, and a result of the inverse affine transformation received the inverse affine transformation circuit, wherein the selected element is selected for encryption, while the result of the inverse affine transformation is selected for decryption, an inverse determining unit obtaining a multiplicative inverse of the selected data byte received from the second selector, an affine transformation circuit applying an affine transformation on the obtained multiplicative inverse, a third selector unit selecting one of two data bytes consisting of the multiplicative inverse received from the inverse determining unit, and a result of the affine transformation received from affine transformation circuit, wherein the result of the affine transformation is selected for decryption, while the multiplicative inverse is selected for encryption, a coefficient table providing first to fourth coefficients in response to the row index, first to fourth ~~Galois field multiplexers~~ Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of the substitution value with first to fourth coefficients, respectively, and an accumulator which accumulates the first to fourth products to develop first to fourth elements of a designated column of a resultant state.

Please replace the paragraph beginning on line 20 of page 18 with the following amended paragraph:

In still another aspect of the present invention, an AES processor is provided which is adapted to an AES instruction including first and second operands respectively selecting input and output registers out of a register file, and an immediate operand selecting a row of a state. The AES processor is composed of a first selector unit selecting an element of the state in response the first operand and the immediate operand,

element, a second selector unit selecting one out of two data bytes consisting of the selected element received from the first selector, and a result of the inverse affine transformation received the inverse affine transformation circuit, wherein the selected element is selected for encryption, while the result of the inverse affine transformation is selected for decryption, an inverse determining unit obtaining a multiplicative inverse of the selected data byte received from the second selector, an affine transformation circuit applying an affine transformation on the obtained multiplicative inverse, a third selector unit selecting one of two data bytes consisting of the multiplicative inverse received from the inverse determining unit, and a result of the affine transformation received from affine transformation circuit, wherein the result of the affine transformation is selected for decryption, while the multiplicative inverse is selected for encryption, first to fourth ~~Galois field multiplexers~~ Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of the substitution value with first to fourth coefficients, respectively, and a storing unit for storing the first to fourth products into the output register selected by the second operand.

Please replace the paragraph beginning on line 6 of page 40 with the following amended paragraph: AP 7-14-10

The ~~Galois field multiplexers~~ Galois field multipliers 107_0 to 107_3 respectively receive the coefficients d_0 to d_3 from the auxiliary register 406, and compute the produces of the selected byte (or element) with the corresponding coefficients. The computed products constitute resultant four-byte data, and the four-byte data is stored in the result register 408. The four-byte data stored in the result register 408 is selected by the write multiplexer 412 and transferred to the output register rt, which is selected from among the registers within the register file 401 by the operand rt received from the decoder 403.